FOR THE GENERAL COUNSEL'S DESK: MANAGING ENFORCEMENT RISKS INVOLVING COOKIES, PIXELS, AND OTHER TRACKING TECHNOLOGIES

Data governance is a mission-critical issue for every company and institution in the United States.

GCs face a host of pressing cybersecurity concerns. Triaging them requires time, attention, and a well-rounded strategy that considers emerging enforcement trends, business needs, and security measures. This approach gives organizations the best chance to proactively implement privacy and security upgrades before compliance risks take root.

The use of cookies, pixels, and other tracking technologies is among the highest risk issues for many organizations, particularly health companies. This is due to the following:

1. The enactment of new laws that heavily regulate such activity, including new state privacy laws in California, Colorado, and Washington that require obtaining opt-in and/or opt-out consent and which do *not* fully exempt Health Insurance Portability and Accountability Act (HIPAA)-covered entities.
2. Significant regulator enforcement and Congressional inquiries, along with new guidance under existing laws (HIPAA, Federal Trade Commission Act, etc.).
3. Widespread litigation alleging such technologies enable unauthorized uses/disclosures of health information.

Complying with these new rules is legally and technologically complex, but it is very easy for regulators, watchdogs, plaintiffs' lawyers, and journalists to immediately identify and sound the alarm on noncompliance by viewing a company's public website and apps—often before the company's legal department identifies these issues.

Examples of recent enforcement actions, litigation and reputational harm are below, but the bottom line is this:

1. The costs to respond to even a minor regulator inquiry or litigation are substantial (they would cost many times more than the cost to comply), particularly given that many laws permit statutory damages even absent a showing of harm.
2. There is widespread, active enforcement, so these risks are considerable and real (rather than remote, speculative or unlikely).
3. Honest missteps and mistakes happen, but companies acting in good faith can still be painted in a bad light. This exposes organizations to damaging reputational harm.
4. These risks are not going away. They are only increasing.

FEDERAL ENFORCEMENT

Both the US Department of Health and Human Services Office for Civil Rights (OCR) and the Federal Trade Commission (FTC) have issued guidance, sent companies warnings/inquiry letters, and commenced enforcement.

- **Joint OCR/FTC Letter (July 2023):** The OCR and the FTC sent a joint letter to approximately 130 hospital systems and telehealth providers warning them about "serious privacy and security risks related to the use of online tracking technologies." As explained in the press release, the OCR warns that if covered entities or business associates have tracking technologies on their websites or mobile apps, they could be impermissibly disclosing consumers' protected health information (PHI) to third parties in violation of HIPAA.
- **OCR Bulletin (December 2022):** The OCR released a bulletin confirming that tracking technologies may collect and disclose PHI in many cases (*e.g.*, when used on authenticated websites after a member logs in). Most companies that provide third-party trackers will not execute business associate agreements, creating a HIPAA breach risk. The guidance also made clear that using technologies on general informational pages is less likely to be PHI. However, any non-PHI data will be subject to relevant, generally applicable state privacy laws that impose an entirely different set on onerous requirements when using such technologies.
- **OCR Audits/Inquiries (Ongoing):** The OCR continues to investigate covered entities' use of tracking technologies. These investigations incur significant costs; legal fees and business interruption can cost companies six to seven figures (often far more than the amount of any fine or settlement). Investigations can also result in public distrust and reputational harm if publicized.
- **FTC Enforcement (Ongoing)**: The FTC remains busy with several enforcement actions under both the Personal Health Records Rule and Section 5 of the FTC Act (see here and here).

STATE ENFORCEMENT

- The California attorney general published numerous examples of enforcement actions, which include actions against health companies.
- Colorado recently commenced enforcement. The announcement mentions warnings and educational letters, but McDermott has health clients that have already received letters alleging noncompliance and commencing investigative action.
- The Washington My Health My Data Act, which would apply to the non-PHI health information that tracking technologies collect, takes effect in a few months and will create a private cause of action as well.

LITIGATION

- Class actions are increasingly being filed against health companies alleging impermissible sharing of health data for marketing purposes. Complaints will often expressly cite the OCR bulletin to establish negligence, breach of contract, and other claims. Many of these cases rely on novel arguments under laws that permit private causes of action seeking statutory damages, such as state wiretapping laws.
- Both the California Consumer Privacy Act and the California Confidentiality of Medical Information Act likewise create a private cause of action for data breaches involving medical or health insurance information. These breaches incur statutory damages of $750 and $1,000/person, respectively, which provide an easy basis to establish a class and survive a motion to dismiss.

As an example, Partners Healthcare System/Mass General reached a **$18.4 million settlement** with a class of Massachusetts residents over the use of cookies, pixels, website analytics tools, and associated technologies on several websites without first obtaining the consent of website visitors.

REPUTATIONAL HARM

- Several high-profile news articles outed companies and described their pixel and data tracking activities. These articles created a distorted narrative that incorrectly suggested these companies' practices were materially different and more offensive compared to other similar companies and the overall ecosystem.
- Pixel and data tracking technologies are complicated, as are the advertising algorithms that may—and equally importantly *may not*—use certain information ingested through such technologies. Industry self-regulatory organizations (such as the Digital Advertising Alliance and Network Advertising Initiative) and newly enacted state privacy laws require consent to the use of sensitive health information for targeted advertising. While not fail-safe, this piece of the privacy puzzle gets lost in headline-grabbing concerns about privacy. This makes it difficult for many companies—particularly those identified in high-profile articles—to engage in a nuanced and balanced conversation about data tracking technologies, actual harm, and whether there is true disclosure risk.

DON'T DO NOTHING

Pixels and data tracking technologies are complicated and difficult to understand. And, they do not fit neatly under the privacy and security rubrics drafted for a different era, like HIPAA. No doubt, some general counsels, chief compliance officers, and other privacy and security professionals are being asked tough questions about whether these trends will simply "blow over" and if "doing nothing" is the most prudent course. While the prospect of tackling pixels and data tracking technology compliance is complex, the cost of doing nothing and facing enforcement, litigation, and/or public scrutiny is a much costlier data governance problem and public relations challenge.

We're here to help implement the necessary data governance to reduce these significant compliance risks. To learn more or discuss your organization's needs, please contact your regular McDermott lawyer or a member of the Firm's integrated data-tracking response team.

INTEGRATED DATA-TRACKING RESPONSE TEAM

STEPHEN W. BERNSTEIN
Partner | Boston
sbernstein@mwe.com
Tel +1 617 535 4062

PURNIMA BOOMINATHAN
Partner | Washington, DC
pboominathan@mwe.com
Tel +1 202 756 8191

DAVID QUINN GACIOCH
Partner | Boston
dgacioch@mwe.com
Tel +1 617 535 4478

JENNIFER S. GEETTER
Partner | Washington, DC
jgeetter@mwe.com
Tel +1 202 756 8205

ELLIOT R. GOLDING
Partner | Washington, DC
egolding@mwe.com
Tel +1 202 756 8185

DANIEL F. GOTTLIEB
Partner | Chicago
dgottlieb@mwe.com
Tel +1 312 984 6471

RYAN S. HIGGINS
Partner | Chicago
rshiggins@mwe.com
Tel +1 312 984 2052

AMY C. PIMENTEL
Partner | Boston
apimentel@mwe.com
Tel +1 617 535 3948

ALYA SULAIMAN
Partner | Los Angeles
asulaiman@mwe.com
Tel +1 310 788 6017

EDWARD G. ZACHARIAS
Partner | Boston
ezacharias@mwe.com
Tel +1 617 535 4018